PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-265217

(43)Date of publication of application : 28.09.2001

(51)Int.Cl. G09C 1/00
G06F 12/14

(21)Application number : 2000-076967

(22)Date of filing : 17.03.2000

(71)Applicant : CTI CO LTD

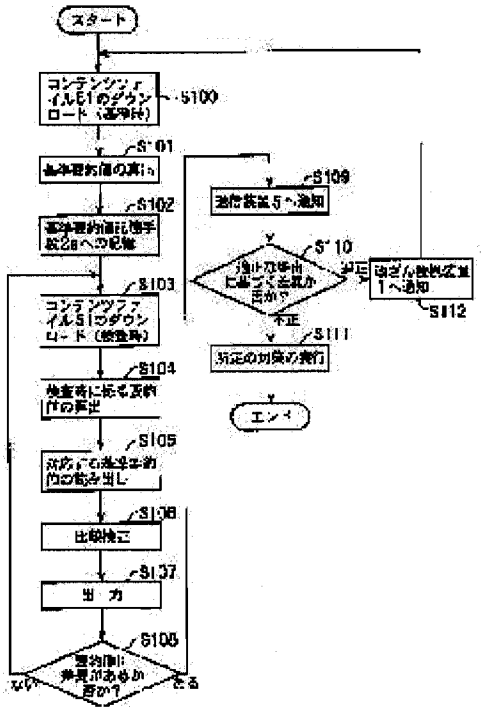
(72)Inventor : SUZUKI SHUNYO
MURASE SHINJI
SUGIE OSAMU

(54) DEVICE AND METHOD FOR MONITORING ALTERATION OF DIGITAL CONTENTS, AND RECORDED MEDIUM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To call attention to whether or not a change in digital contents is unauthorized, by speedily detecting the change in the digital contents and outputting the result for notification.

SOLUTION: A summed-up value calculating means for calculating a summed-up value of a content file related to digital contents to be monitored by a unidirectional function, is provided, a summed-up value at the reference time and that at the inspection time are compared with each other. Therefore, it is possible to detect at an early stage the fact of a change in the contents. By outputting the verification result of the comparison and notifying the information supplier of the digital contents to be monitored thereof, it is possible to call their attention to whether the change is unauthorized, and prevent the scale of damage from expanding. Moreover, since any change is being monitored by using a summed-up value by a unidirectional function, comparison verification can be performed speedily.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－265217
（P2001－265217A）
(43)公開日　平成13年９月28日(2001.9.28)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｂ０１７
			６４０Ｚ	５Ｊ１０４
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ	９Ａ００１

審査請求　未請求　請求項の数12　ＯＬ　（全　９　頁）

(21)出願番号　特願2000－76967(P2000－76967)

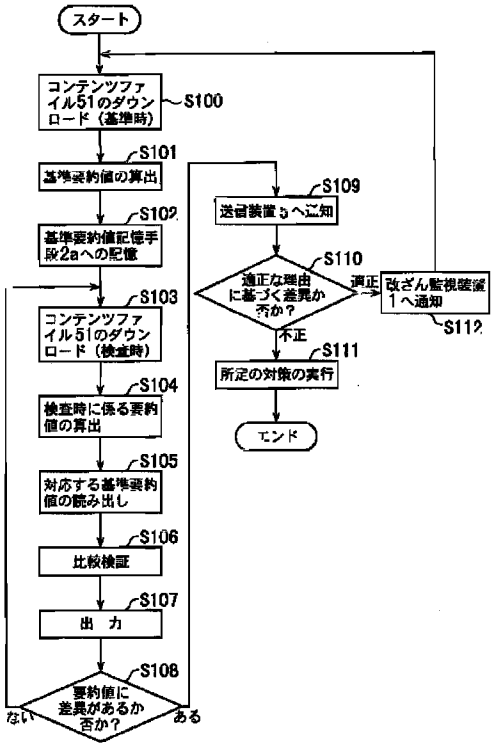
(22)出願日　平成12年３月17日(2000.3.17)

(71)出願人　599103850
株式会社シーティーアイ
愛知県名古屋市中村区名駅南一丁目27番２号
(72)発明者　鈴木　春洋
愛知県名古屋市中村区名駅南一丁目27番２号　株式会社シーティーアイ内
(72)発明者　村瀬　晋二
愛知県名古屋市中村区名駅南一丁目27番２号　株式会社シーティーアイ内
(74)代理人　100073139
弁理士　千田　稔　（外１名）

最終頁に続く

(54)【発明の名称】　デジタルコンテンツの改ざん監視装置、改ざん監視方法及び記録媒体

(57)【要約】
【課題】　デジタルコンテンツの内容変更を速やかに発見し、その結果を出力して知らせることで、不正な改ざんによるものか否かの注意を喚起する。
【解決手段】　監視対象となるデジタルコンテンツに係るコンテンツファイルの、一方向関数による要約値を算出する要約値算出手段を設定し、基準時に係る要約値と検査時に係る要約値とを比較する。従って、内容が変更された事実を早期に発見できる。比較検証結果を出力して監視対象となっているデジタルコンテンツの情報提供者に知らせることで、不正な改ざんによるものか否かの注意を喚起でき、被害規模の拡大を防ぐことができる。また、一方向関数による要約値を用いて監視しているため、比較検証を迅速に行うことができる。



【特許請求の範囲】
【請求項１】　ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視装置であって、
監視対象となるデジタルコンテンツに係るコンテンツファイルの、一方向関数による要約値を算出する要約値算出手段と、
前記要約値算出手段により算出した前記デジタルコンテンツの基準時に係るコンテンツファイルの要約値が、基準要約値として記憶されている記憶手段と、
前記要約値算出手段により算出した前記デジタルコンテンツの検査時に係るコンテンツファイルの要約値を、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する比較検証手段と、
前記比較検証手段による検証結果を出力する出力手段とを具備することを特徴とするデジタルコンテンツの改ざん監視装置。
【請求項２】　請求項１記載のデジタルコンテンツの改ざん監視装置であって、前記送信装置がウエブサーバであり、前記デジタルコンテンツがウエブページであることを特徴とするデジタルコンテンツの改ざん監視装置。
【請求項３】　請求項１又は２記載のデジタルコンテンツの改ざん監視装置であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とするデジタルコンテンツの改ざん監視装置。
【請求項４】　請求項１～３のいずれか１に記載のデジタルコンテンツの改ざん監視装置であって、前記基準要約値を用いた電子署名が付加されて記憶されていることを特徴とするデジタルコンテンツの改ざん監視装置。
【請求項５】　監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、記憶手段に基準要約値として記憶させるステップと、
前記デジタルコンテンツの検査時に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証するステップと、
前記ステップによる検証結果を出力するステップとを具備し、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体。
【請求項６】　請求項５記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記送信装置がウエブサーバであり、前記デジタルコンテンツがウエブページであることを特徴とする記録媒体。
【請求項７】　請求項５又は６記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする記録媒体。
【請求項８】　請求項５～７のいずれか１に記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記記憶手段に基準要約値を記憶させるステップにおいては、当該基準要約値の電子署名を作成し、当該電子署名を付加して記憶させるように設定されることを特徴とする記録媒体。
【請求項９】　ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視方法であって、
監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、コンピュータの記憶手段に基準要約値として記憶させる工程と、
前記デジタルコンテンツの検査時に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する工程と、
前記ステップによる検証結果を出力する工程とを具備することを特徴とするデジタルコンテンツの改ざん監視方法。
【請求項１０】　請求項９記載のデジタルコンテンツの改ざん監視方法であって、前記送信装置がウエブサーバであり、前記デジタルコンテンツがウエブページであることを特徴とするデジタルコンテンツの改ざん監視方法。
【請求項１１】　請求項９又は１０記載のデジタルコンテンツの改ざん監視方法であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とするデジタルコンテンツの改ざん監視方法。
【請求項１２】　請求項９～１１のいずれか１に記載のデジタルコンテンツの改ざん監視方法であって、前記記憶手段に基準要約値を記憶させる工程においては、当該基準要約値の電子署名を作成し、当該電子署名を付加して記憶させるものであることを特徴とするデジタルコンテンツの改ざん監視方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタルコンテンツの改ざん監視装置、監視方法及びデジタルコンテンツの改ざん監視をコンピュータに実行させるための記録媒体に関する。
【０００２】
【従来の技術】近年、コンピュータネットワークの急速な普及により、インターネットのウエブページなどの形式で、不特定多数を対象に公開されるデジタルコンテンツが多くなってきている。

【0003】
【発明が解決しようとする課題】しかしながら、同時にまた、例えば、WWW (World Wide Web) 上の送信サーバ (送信装置) への不正アクセスなどによって、ウエブページ (ホームページ) の内容が改ざんされる事故も増加している。
【0004】本発明は上記した点に鑑みなされたものであり、ウエブページのような不特定多数を対象に提供されるデジタルコンテンツの内容変更を速やかに発見し、その結果を出力して知らせることで、不正な改ざんによるものか否かの注意を喚起できるデジタルコンテンツの改ざん監視装置、監視方法及びデジタルコンテンツの改ざん監視をコンピュータに実行させるための記録媒体に関する。
【0005】
【課題を解決するための手段】上記課題を解決するため、請求項1記載の本発明のデジタルコンテンツの改ざん監視装置は、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視装置であって、監視対象となるデジタルコンテンツに係るコンテンツファイルの、一方向関数による要約値を算出する要約値算出手段と、前記要約値算出手段により算出した前記デジタルコンテンツの基準時に係るコンテンツファイルの要約値が、基準要約値として記憶されている記憶手段と、前記要約値算出手段により算出した前記デジタルコンテンツの検査時に係るコンテンツファイルの要約値を、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する比較検証手段と、前記比較検証手段による検証結果を出力する出力手段とを具備することを特徴とする。
【0006】請求項2記載の本発明のデジタルコンテンツの改ざん監視装置は、請求項1記載のデジタルコンテンツの改ざん監視装置であって、前記送信装置がウエブサーバであり、前記デジタルコンテンツがウエブページであることを特徴とする。
【0007】請求項3記載の本発明のデジタルコンテンツの改ざん監視装置は、請求項1又は2記載のデジタルコンテンツの改ざん監視装置であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする。
【0008】請求項4記載の本発明のデジタルコンテンツの改ざん監視装置は、請求項1～3のいずれか1に記載のデジタルコンテンツの改ざん監視装置であって、前記基準要約値を用いた電子署名が付加されて記憶されていることを特徴とする。
【0009】請求項5記載の本発明の記録媒体は、デジタルコンテンツの改ざん監視装置は、監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、記憶手段に基準要約値として記憶させるステップと、前記デジタルコンテンツの検査時に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証するステップと、前記ステップによる検証結果を出力するステップとを具備し、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録したことを特徴とする。
【0010】請求項6記載の本発明の記録媒体は、請求項5記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記送信装置がウエブサーバであり、前記デジタルコンテンツがウエブページであることを特徴とする。
【0011】請求項7記載の本発明の記録媒体は、請求項5又は6記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする。
【0012】請求項8記載の本発明の記録媒体は、請求項5～7のいずれか1に記載のネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視をコンピュータに実行させるプログラムを記録した記録媒体であって、前記記憶手段に基準要約値を記憶させるステップにおいては、当該基準要約値の電子署名を作成し、当該電子署名を付加して記憶させるように設定されることを特徴とする。
【0013】請求項9記載の本発明のデジタルコンテンツの改ざん監視方法は、ネットワークを介して送信装置により提供されるデジタルコンテンツの改ざん監視方法であって、監視対象となるデジタルコンテンツの基準時に係るコンテンツファイルの、一方向関数による要約値を算出し、コンピュータの記憶手段に基準要約値として記憶させる工程と、前記デジタルコンテンツの検査時に係るコンテンツファイルの、一方向関数による要約値を算出し、前記記憶手段から読み出した基準要約値と比較し、両者の差異を検証する工程と、前記ステップによる検証結果を出力する工程とを具備することを特徴とする。
【0014】請求項10記載の本発明のデジタルコンテンツの改ざん監視方法は、請求項9記載のデジタルコンテンツの改ざん監視方法であって、前記送信装置がウエブサーバであり、前記デジタルコンテンツがウエブページであることを特徴とする。
【0015】請求項11記載の本発明のデジタルコンテンツの改ざん監視方法は、請求項9又は10記載のデジタルコンテンツの改ざん監視方法であって、前記一方向関数がハッシュ関数であり、前記要約値がハッシュ値であることを特徴とする。
【0016】請求項12記載の本発明のデジタルコンテ

ンツの改ざん監視方法は、請求項９～１１のいずれか１に記載のデジタルコンテンツの改ざん監視方法であって、前記記憶手段に基準要約値を記憶させる工程においては、当該基準要約値の電子署名を作成し、当該電子署名を付加して記憶させるものであることを特徴とする。

【００１７】

【発明の実施の形態】以下、本発明を図面に示した実施形態に基づいて更に詳しく説明する。図１は、本発明の一の実施形態にかかる改ざん監視装置１の構成図である。この図に示したように、この改ざん監視装置１はコンピュータから構成され、ＣＰＵ、メモリやハードディスクドライブなどの記憶手段２を有すると共に、入出力制御部４を介して接続されたモニタ３などのハードウエアを有し、さらに所定のＯＳがインストールされている。また、本実施形態においてデジタルコンテンツの改ざん監視を行うための制御手段１０として機能するプログラムが記憶手段２にインストールされる。

【００１８】本実施形態の制御手段１０であるプログラムは、一方向関数による要約値を算出する要約値算出手段１１を備えている。要約値算出手段１１は、監視対象となるデジタルコンテンツに係るコンテンツファイルを、一方向関数により要約する手段である。監視対象となるデジタルコンテンツは、複数の端末からアクセスされることによって、自動送信される形態で開示されているものであれば何であってもよく、例えば、ウエブサーバ（送信装置５）によって提供される任意のウエブページ（ホームページ）上の情報が挙げられる。特に、近年、第三者の不正アクセスによるウエブページ（ホームページ）の改ざんが頻出しているので、これを監視対象とすることにより本発明を有効に利用できる。もちろん、パソコン通信等によって提供されるデジタルコンテンツであってもよい。

【００１９】また、このデジタルコンテンツの内容に制限はなく、テキストデータ、画像データ等の種々のデータであってよいが、例えば、日付やアクセスカウンタなどのように常に変化するデータを含めると、それらが変化するだけでも要約値が変化してしまうことから、このようなデータは監視対象となるデジタルコンテンツから除外しておくことが好ましい。

【００２０】上記したデジタルコンテンツに係るコンテンツファイルの入手方法は任意であるが、監視対象とするウエブページの情報提供者（送信装置５の管理者ないしは運営者）と本実施形態の改ざん監視装置１の管理者ないしは運営者との間で契約が結ばれたならば、改ざん監視装置１から監視対象となるウエブページにインターネットを利用してアクセスし、当該監視装置１にコンテンツファイルをダウンロードすることにより入手したり、あるいは、コンテンツファイルを記録したＣＤ－ＲＯＭ、ＤＶＤ、フレキシブルディスクなどの記録媒体を入手して改ざん監視装置１に記憶させることもできる。また、送信装置５に記録されているコンテンツファイル５１を専用回線などによって監視装置１に記憶させることもできる。

【００２１】要約値を算出する具体的な手段としては、典型的には、ハッシュ関数を利用することが好ましい。ハッシュ関数とは、ファイルを一定の長さ（例えば、１２８ビット）のハッシュ値に圧縮する関数であり、変換された文字列から元の文字列を見つけだすことがほとんど不可能な強一方向性であると共に、元の文章が１ビットでも異なれば結果として得られるハッシュ値が大きく変わるという特徴をもっている。ハッシュ関数の種類は限定されるものではなく、例えば、ＭＤ－５、ＭＡＳＨ、米国標準技術局のＳＨＡ－１などを用いることができる（図３参照）。

【００２２】制御手段１０であるプログラムは、また、上記要約値算出手段１１によって、基準時に係るコンテンツファイル５１のハッシュ値を算出して、さらにそれを基準要約値として記憶手段２の一部に形成した基準要約値記憶部２ａに記憶させるステップを備えている。ここで、基準時とは、上記の例でいえば、監視対象となるウエブページの情報提供者との間で契約成立後に、初めてダウンロードする時、あるいは、当該情報提供者が記録媒体の形式でコンテンツファイル５１を提供する場合における当該コンテンツファイル５１の記録媒体への記録時などをいうが、不正な改ざん等がなされていない状態の比較基準となるコンテンツファイル５１を特定した時点であればこれらに限定されるものではない。

【００２３】また、デジタルコンテンツ（ウエブページ）の内容が適正に更新された場合には、更新されたコンテンツファイル５１の要約値を基準とする必要があるため、その際には、更新されたコンテンツファイル５１をダウンロードなどにより特定した時点が基準時となる。

【００２４】また、制御手段１０であるプログラムは、任意の検査タイミングで、例えば、数分おき、数時間おき、毎日所定時刻、数日おきなどのタイミングで、監視対象となっているウエブサーバにアクセスし、所定のデジタルコンテンツ（ウエブページ）のコンテンツファイル５１を記憶手段２にダウンロードし、当該コンテンツファイル５１の要約値を要約値算出手段１１によって算出するステップを有する。すなわち、比較対象となる検査時に係るコンテンツファイル５１の要約値を算出するものである。

【００２５】この検査時に係る要約値を算出したならば、比較検証手段を構成するステップにおいて、予め基準要約値記憶部２ａに記憶されている当該監視対象となっているデジタルコンテンツのコンテンツファイル５１の基準要約値を読み出し、検査時に係る要約値を当該基準要約値と比較し、両者の差異を検証する。このステップにより両者間に差異があった場合には、上記コンテン

ツファイルに係るデジタルコンテンツに何らか原因で変更が生じたことを意味する。

【0026】上記比較検証手段による検証結果は、上記プログラムに組み込まれた出力ステップにより、任意の出力手段を通じて出力される。出力手段は、特に限定されるものではなく、改ざん監視装置1のモニタ3に出力することもできるし、モニタ3と共にプリンタ（図示せず）に出力することもできるし、さらには、モニタ3とプリンタの両者に出力することもできる。また、これらと併用してあるいはこれらと併用せずに、監視対象となっているデジタルコンテンツ（ウエブページ）を提供している送信装置5のハードディスクドライブや半導体メモリ等に対し、任意の通信網を介して出力する構成とすることもできる。任意の通信網とは、本実施形態の改ざん監視装置1と送信装置5とを結ぶ専用回線であってもよいし、パソコン通信やインターネットを利用して、電子メール形態で出力することもできる。

【0027】ここで上記した制御手段10であるプログラムを記録した記録媒体としては、例えば、フレキシブルディスクなどの磁気ディスク、CD-ROM、DVDなどの光ディスク、MO、MDなどの光磁気ディスク、ICカードなどの半導体カード等が挙げられる。また、改ざん監視装置1と通信網を介して接続された任意のコンピュータ（図示せず）のハードディスクドライブ、半導体メモリ等を記録媒体として使用して、通信網を介してプログラムを提供することもできる。また、単一の記録媒体により提供してもよいし、プログラムを複数の記録媒体に分割して格納して提供することもできる。

【0028】次に、本実施形態の改ざん監視装置1を用いた改ざん監視方法の一例を図2のフロー図に基づき説明する。まず、上記したように、予め、監視対象となるデジタルコンテンツ（例えば、ウエブページ）に係るコンテンツファイル51を、改ざん監視装置1の記憶手段2に、例えば、当該ウエブページを提供している送信装置（ウエブサーバ）5にインターネットを通じてアクセスし、ダウンロードする（S100）。この際のウエブページの内容は何らの書き換え、改ざんが行われてないものとし、このコンテンツファイル51のダウンロード時を基準時とする。

【0029】次に、要約値算出手段11により、当該コンテンツファイルのハッシュ値を算出し（S101）、これを基準要約値として、記憶手段2に形成された基準要約値記憶部2aに記憶させる（S102）。

【0030】なお、監視対象となるデジタルコンテンツは、一つであってもよいが、同一の送信装置5が提供している情報中の複数であってもよい。さらには、異なる者によって管理ないし運営されている複数の送信装置5によって提供されている複数の情報を監視対象とすることももちろん可能である。

【0031】基準要約値記憶部2aに記憶されている基準要約値は、ハッシュ関数による圧縮を行う前の生のコンテンツファイル51と対応させて記憶させておくこともできるが、監視対象が複数存在する場合、改ざん監視装置1の負荷を軽減するため、当該デジタルコンテンツの所在情報、例えば、ウエブページであれば、URLと対応させて格納しておくことが好ましい。従って、図3に示したように、本実施形態では、記憶手段2に、監視対象となっている各デジタルコンテンツ（ウエブページ）のURL記憶部2bが格納されており、各URLに対応させて基準要約値を格納している。

【0032】次に、任意のタイミングで、監視対象に係るデジタルコンテンツ（ウエブページ）を再びダウンロードする（S103）。そして、上記と同様に要約値算出手段11によりハッシュ値を算出する（S104）。このハッシュ値は検査時に係る要約値となる。なお、検査時は、監視対象となっているデジタルコンテンツが複数存在する場合、同じタイミングで設定することもできるし、デジタルコンテンツごとに異なるタイミングを設定することもできる。

【0033】次に、検査時に係る要約値を算出したデジタルコンテンツ（ウエブページ）に対応する基準要約値を、URL記憶部2bに記憶されたURLに基づき、基準要約値記憶部2aから読み出す（S105）。そして、検査時に係る要約値とこの基準要約値とを比較検証し、この検証結果を上記した出力手段により出力する（S106～S108）。

【0034】検証した結果、両者に差異がない場合には、再び、任意の検査タイミングで上記工程を繰り返す。一方、検証結果に差異がある場合には、例えば、改ざん監視装置1のモニタ3やプリンタに検証結果を出力したならば、改ざん監視装置1の管理者ないしは運営者が、その旨を上記デジタルコンテンツ（ウエブページ）を提供している送信装置5の管理者ないしは運営者（情報提供者）に連絡する（S109）。連絡手段としては、電話、ファクシミリ、電子メール等が挙げられるがこれに限定されるものではない。連絡を受けた送信装置5の管理者等は、その差異が、適正な更新作業に基づくものか、不正アクセスによる改ざんに基づくものかを検証する（S110）。その結果、不正アクセスによる改ざんに基づくものである場合には、デジタルコンテンツ（ウエブページ）の送信を停止するなどして、所定の対策をとる（S111）。このように、本実施形態によれば、改ざん監視装置1により、デジタルコンテンツ（ウエブページ）の内容が定期的、あるいは適宜のタイミングで監視されているため、第三者による不正な改ざんを早期に発見し、被害規模の拡大を防ぐことができる。

【0035】一方、上記の検証結果の差異が、適正な更新作業に基づくものである場合には、送信装置5の管理者等は、電話、ファクシミリ、電子メールなどを通じて、改ざん監視装置1の管理者等に連絡する（S11

2)。改ざん監視装置1の管理者等は、この連絡を受けたならば、改めて、ウエブページにアクセスし、新たに基準となるコンテンツファイル51をダウンロードし、ハッシュ値を算出して、当該ウエブページのURLに対応する基準要約値を更新する。なお、この場合、改ざん監視装置1において、例えば電子メールにより適正な更新作業に基づくものである旨の通知を受信したならば、上記ウエブページへのアクセス及び新たに基準となるコンテンツファイル51のダウンロードを自動的に行うように制御手段10をプログラミングしておくこともできる。

【0036】また、検証結果に差異が生じた場合、改ざん監視装置1の管理者等による人の連絡作業を介在させずに、ファクシミリやメールクライアント等を自動起動し、その結果を監視対象となっているデジタルコンテンツ(ウエブページ)を提供している送信装置5に対し、自動的に送信されるように制御手段10をプログラミングし、当該送信装置5のハードディスクドライブ等に直接出力することもできる。

【0037】また、図4に示したように、比較検証の結果、要約値に差異があった場合には、送信装置5に通知する際に(S109)、送信装置5の管理者等が改ざんを確認するに当たってアクセスすべきURLを付加(S109a)して送ることが好ましい。これにより、送信装置5の管理者等における確認作業が容易となる。

【0038】この場合、付加するURLとしては、監視対象となっているウエブページ(デジタルコンテンツ)のURLと、本実施形態の改ざん監視装置1にアクセスするためのURLが考えられるが、前者の場合には、送信装置5の管理者等は、確認後、その旨を改ざん監視装置1へ別途通知(S112)する必要がある。一方、後者の場合には、例えば、図5に示したように、改ざん監視装置1にアクセスすると、内容変更が行われたウエブページ(デジタルコンテンツ)の内容(又はリンク用のURL)と共に、「改ざんされているか否か(不正か適正か)」を判断して入力できるメニューを予め用意しておくことにより、「適正」のボタンを押すだけで、上記実施形態における「改ざん監視装置1への通知(S112)」工程を容易かつ自動的に行うことができる。

【0039】また、図6に示したように、基準要約値の算出ステップ(S101)を経たならば、基準要約値に対して、必要に応じてタイムスタンプを付加した後、改ざん監視装置1が有している秘密鍵を用いて電子署名を作成することもできる(S101a)。そして、基準要約値を基準要約値記憶部2aに記憶させると共に、この電子署名に係る暗号文も記憶手段2に形成した電子署名記憶部2cに記憶させる(S102')。従って、記憶手段2においてファイル又はテーブルの形式で設定される各記憶部2a,2b,2cの構成は、例えば、図7に示したようになる。

【0040】このようにして電子署名も作成した場合には、比較検証ステップ(S106)においては、まず、改ざん監視装置1の公開鍵により、電子署名を復号化し(S106a)、その復号文から得られる基準要約値を基準要約値記憶部2aの基準要約値と比較する(S106b)。両者が一致していれば、基準要約値と検査時に係る要約値とを比較検証する(S106c)。電子署名を作成していない場合には、改ざん監視装置1自体へ不正アクセスした第三者が要約値を書き換えたとしてもその事実を発見することが困難であるが、このように電子署名を作成しておくことにより、基準要約値の書き換え等が行われた否かも検出することができる。従って、比較検証ステップ(S106)において用いる基準要約値は信頼性のあるものとなる。

【0041】なお、上記した電子署名の作成に当たっては、基準要約値に対してそのまま電子署名していたが、さらに、第三者による不正な書き換え等の防止効果を高めるため、基準要約値のダイジェスト(例えば、ハッシュ関数を用いたハッシュ値)を作成し、そのダイジェストに対して、必要に応じてタイムスタンプを付加し、秘密鍵により電子署名することもできる。

【0042】さらに、改ざん監視装置1自体への第三者の不正アクセスを確実に発見する手段として、基準要約値及び/又は電子署名を、基準要約値の算出時及び/又は基準要約値記憶部2aへの基準要約値の記録時、電子署名を作成した場合には電子署名の作成時及び/又は電子署名記憶部2cへの記録時と共に、別途履歴管理しておくことが好ましい。これにより、不正アクセスが介在した場合には、その事実をより確実かつ容易に発見できる。

【0043】この場合、基準要約値及び/又は電子署名に関する上記の各算出時及び/又は記録時の時刻を保証するため、それらのデータに電子署名を行って管理するタイムスタンプサーバ(図示せず)を利用することがさらに好ましい。タイムスタンプサーバによる電子署名は、改ざん監視装置とは別途のタイムスタンプサーバ独自の秘密鍵を用いて電子署名するため、安全性が高まる。また、タイムスタンプサーバは、改ざん監視装置1と同一のコンピュータ内に設定することも可能であるが、別のコンピュータに設定しておくことが安全性の点から好ましい。

【0044】

【発明の効果】本発明のデジタルコンテンツの改ざん監視装置、改ざん監視方法及び記録媒体によれば、デジタルコンテンツを任意のタイミングで検査し監視しているため、内容が変更された事実を早期に発見できる。従って、比較検証結果を出力して監視対象となっているデジタルコンテンツの情報提供者に知らせることで、不正な改ざんによるものか否かの注意を喚起でき、被害規模の拡大を防ぐことができる。また、一方向関数による要約

値を用いて監視しているため、比較検証を迅速に行うことができる。特に、ハッシュ関数を用いた場合には、監視対象のデジタルコンテンツの内容が少しでも異なれば結果として得られるハッシュ値が大きく変わるため、比較検証を確実に行うことができる。

【図面の簡単な説明】

【図１】図１は、本発明の一の実施形態にかかる改ざん監視装置を示す構成図である。

【図２】図２は、本発明の一の実施形態にかかる改ざん監視方法を説明するためのフロー図である。

【図３】図３は、上記実施形態にかかる改ざん監視装置の記憶手段に形成される基準要約値記憶部及びＵＲＬ記憶部の概略構成を示す図である。

【図４】図４は、他の態様に係る改ざん監視方法において、上記実施形態の改ざん監視方法と相違する点を示したフロー図である。

【図５】図５は、図４のＳ１０９ａにおいて付加したＵＲＬにアクセスして表示された状態の一例を示す図である。

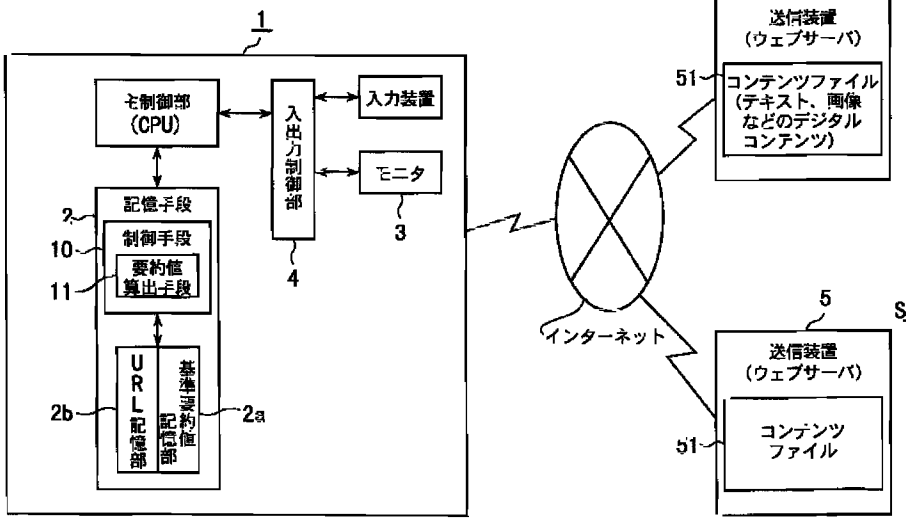
【図６】図６は、さらに他の態様に係る改ざん監視方法において、上記実施形態の改ざん監視方法と相違する点を示したフロー図である。

【図７】図７は、上記他の態様に係る改ざん監視装置の記憶手段に形成される基準要約値記憶部、ＵＲＬ記憶部及び電子署名記憶部の概略構成を示す図である

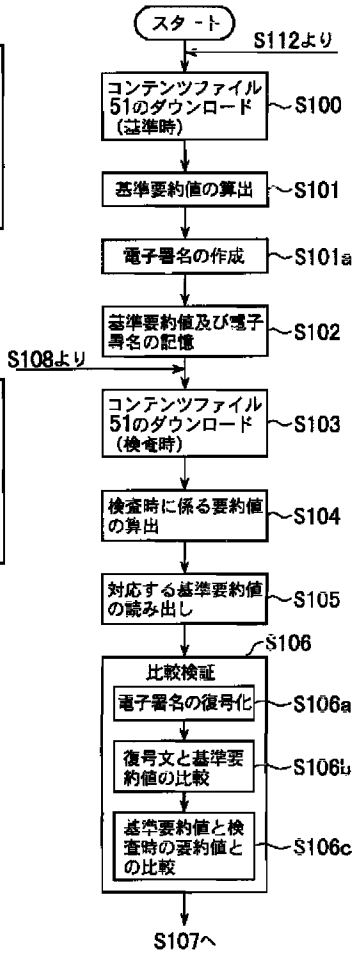
【符号の説明】

１　改ざん監視装置
２　記憶手段
１０　制御手段
１１　要約値算出手段
２ａ　基準要約値記憶部
２ｂ　ＵＲＬ記憶部
２ｃ　電子署名記憶部
５　送信装置
５１　コンテンツファイル

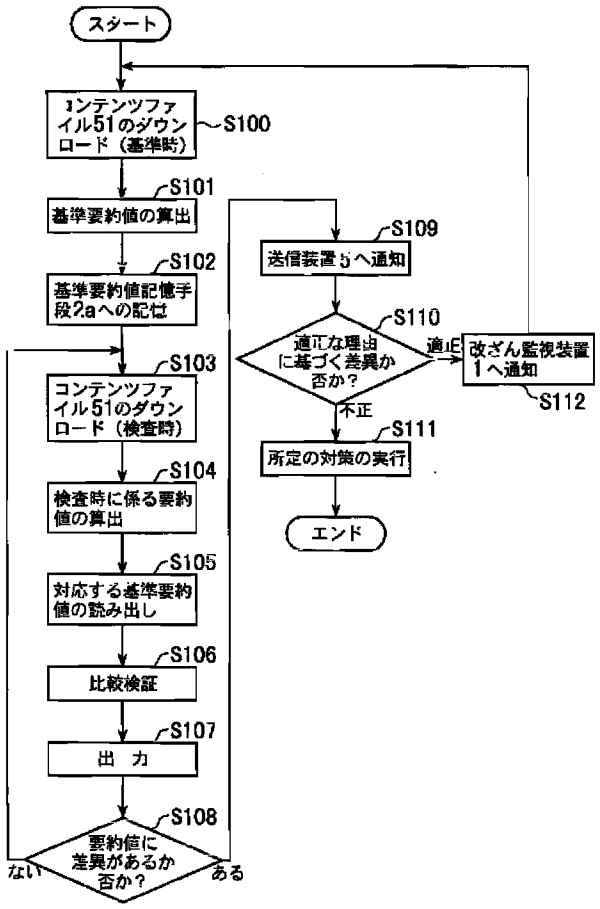
【図１】



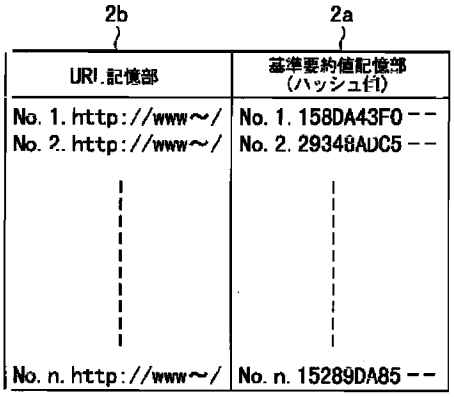
【図６】



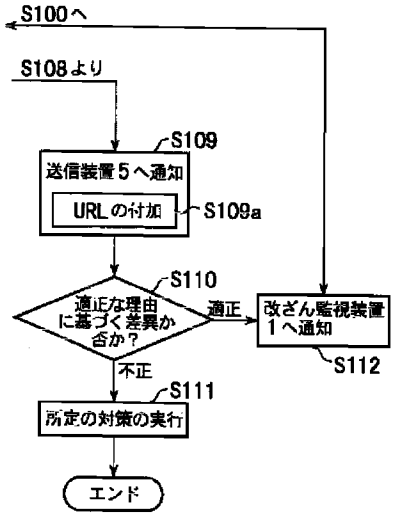
【図2】


スタート
コンテンツファイル51のダウンロード（基準時）
S100
基準要約値の算出
S101
基準要約値記憶手段2aへの記憶
S102
コンテンツファイル51のダウンロード（検査時）
S103
検査時に係る要約値の算出
S104
対応する基準要約値の読み出し
S105
比較検証
S106
出力
S107
要約値に差異があるか否か？
S108
ない
ある
送信装置5へ通知
S109
適正な理由に基づく差異か否か？
S110
適正
改ざん監視装置1へ通知
S112
不正
所定の対策の実行
S111
エンド

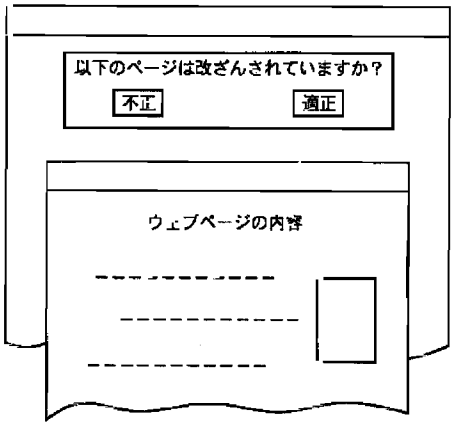
【図3】


2b
2a
URL記憶部
基準要約値記憶部（ハッシュ値）
No. 1. http://www～/
No. 1. 158DA43F0 - -
No. 2. http://www～/
No. 2. 29348ADC5 - -
No. n. http://www～/
No. n. 15289DA85 - -

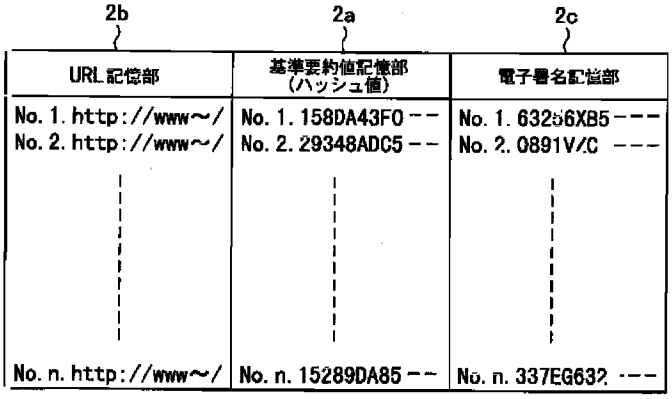
【図4】


S100へ
S108より
送信装置5へ通知
S109
URLの付加
S109a
適正な理由に基づく差異か否か？
S110
適正
改ざん監視装置1へ通知
S112
不正
所定の対策の実行
S111
エンド

【図5】


以下のページは改ざんされていますか？
不正
適正
ウェブページの内容

【図7】



フロントページの続き

(72)発明者 杉江 修
愛知県名古屋市中村区名駅南一丁目27番2号 株式会社シーティーアイ内

Fターム(参考) 5B017 AA08 BA09 BB02 CA16
5J104 AA08 AA09 LA01 LA05 LA06
NA11 NA12 NA27 PA07 PA09
9A001 BB02 BB03 BB04 CC02 DD09
EE02 EE03 GG21 JJ13 JJ25
JJ27 JJ67 JZ14 KK42 KK43
KK60 LL03